State of Wisconsin
Department of Administration
Division of Enterprise Technology

SECURITY

Effective Date: 7/1/17

Incident Response Standard

Purpose

The Incident Response standard defines an information security incident(s) for Division of Enterprise Services, DET/State IT systems and system environments. It also documents the associated requirements to achieve compliance with the following policies and standards:

- Audit and Compliance Policy and Standard
- Configuration Management Policy and Standard
- Contingency Planning Policy and Standard
- Incident Response Policy
- Risk Assessment Policy and Standard
- System and Communication Policy and Standard

Standard

Any DET/State IT system and/or system environment, including IT services and equipment, could be affected by an information security incident. Documented, tested, and practiced incident response procedures must be implemented to address potential or known information security incidents, (IR-2, IR-3).

This standard utilizes the NISTIR-7298 Rev. 2 definition of an information security incident, which states:

> "An (information security) incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An (information security) incident is also defined as any event that adversely affects the confidentiality, integrity, or availability of system(s) and its data."

The following elements must be included in any DET/State information security incident response procedure:

When to report

All DET employees, contractors, vendors, customers, and/or interns are to report any known or suspected information security events or incidents as soon as possible to DET Security via the Enterprise Service Desk at (608) 264-9383 or esdhelp@wi.gov (IR-7).

Please note: If there are questions/concerns about if a situation is a security event/incident or not, please contact DET Security via the ESD Desk at (608) 264-9383 or esdhelp@wi.gov to discuss (IR-7).

Effective Date: 7/1/17

What to report

Known or suspected information security incidents must be reported to DET Security via the ESD Desk at (608) 264-9383 or esdhelp@wi.gov. If possible, please be prepared to provide the following information (IR-7):

- Reporting person's name and contact information, including affected agency/department information;
- Description of event/incident;
- Type of device/system/service affected;
- Date/time incident occurred;
- Date/time incident discovered;
- How many records/files affected;
- Was any personally identifiable information, PII, affected by the event/incident?
- Equipment/website affected by the event/incident; and,
- Was the device/information encrypted?

Steps for Incident Handling

Pre-incident handling

- Determine required incident response roles (e.g. technical, informational, coordinator, audit/legal) *(IR-4)*.
- Identify personnel who will fill the incident response roles and maintain a current list of names and contact information for those individuals *(IR-4)*.
- Train personnel in their specific incident response roles (IR-2, IR-4), Note*: Individuals serving in incident response roles must have appropriate account access, authorization and training to fulfill their assigned roles.*
- Develop an incident response communications plan including *(IR-4)*:
    - Reminder to all incident response members to keep information confidential and to share incident-related information on a need to know basis
    - Determine confidential methods of communication to be used between/among the incident response team and other stakeholders
    - Plan the timing of regular communication/updates to stakeholders during incident response.
    - Develop standard forms and/or formats to gather and report incident information to facilitate effective record keeping and sharing of information.
- Document steps to address basic information security incidents, e.g. phishing, malware, information spillage, equipment theft/loss, copyright infringements *(IR-4)*.

During incident handling (IR-4)

- Determine the level of incident response required based on the Functional Impact Categories, see Table-1.

Table 1 – Functional Impact Categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users or there is a disclosure of information categorized as classified or restricted, as defined by the Data Classification Standard.

Adapted from NIST 800-61 Rev. 2

- Assign individuals to incident response roles *(IR-4)*.
- Investigate the incident, perform analysis and mitigate the issue, perform recovery actions to return system/environment to a functional state *(IR-4)*.
  Note: Use standard forms/formats to document all relevant investigation (including forensics), mitigation, and recovery actions associated with the incident for audit and/or future planning/training efforts (IR-4, IR-5, IR-7).
- Communicate with stakeholders according to communication plan and schedule *(IR-4)*.
- If needed, coordinate incident response with applicable contingency plans, continuity of operations plans (COOP) and/or disaster recovery plans (IR-4).
- If an information security/IT security incident is determined to be a data breach, as defined by the DOA Legal team, the DET Data Breach procedures must be followed.

Post incident handling

- Conduct and document an after-action review. Including on-going remediation plans, lessons learned and next steps/suggested changes, if needed *(IR-4)*.
- Review/update/change incident response plans/training to address identified needs *(IR-4).*

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to, network

devices, servers, databases, printers, Internet, email, physical, virtual, and applications accessible to and/or managed by DET.

- Information security/IT security breach – An incident that results in the confirmed disclosure (not just potential exposure) of confidential data or restricted data (as defined in the Data Classification Standard) to an unauthorized party.
- Information security/IT security event(s) – Any observable occurrence in a network and/or system (NISTIR 7298, Rev. 2). *Note: There can be many types of events but only this criterion identifies an event as an information security event*.
- Information security/IT security incident(s) - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. A computer security incident is also defined as any event that adversely affects the confidentiality, integrity, or availability of system(s) and its data (NISTIR 7298, Rev. 2).
- Information spillage - Instances where either classified or sensitive information is inadvertently placed on information systems/areas that are not authorized to process such information (NIST 800-53 Rev. 4).
- Personally identifiable information, PII – Information which can be sued to distinguish or trace the identity of an individual (e.g. name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g. date and place of birth, mother's maiden name, etc.) (NIST 800-53 Rev. 4).

Compliance/Policy References

CJIS
HIPAA
IRS Pub. 1075
NIST 800-53 Version 4

Exception Process

Exceptions to this and all DET Security policies procedures must follow the DET Exception Procedure.

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

State of Wisconsin
Department of Administration
Division of Enterprise Technology

SECURITY

Effective Date: 7/1/17

Version	Approval/Revision/Review Date	Description	Approver/Author, Title
.1	4/1/2016	draft	Jeff Thompson
.2	7/5/2016	Revisions and updates	Tanya Choice Cybersecurity Compliance Consultant
1.	6/26/17	Final Approval	Bill Nash CISO

Authorized and Approved by:

Bill Nash	Bill Nash	6/26/17
Print/Type	Signature	Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer